UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/725,821	11/29/2000	James D. Dworkin	SC11015ZC	4735

23125 7590 06/22/2004

FREESCALE SEMICONDUCTOR, INC.
LAW DEPARTMENT
7700 WEST PARMER LANE MD:TX32/PL02
AUSTIN, TX 78729

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	**PAPER NUMBER**
2131	2

DATE MAILED: 06/22/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/725,821	DWORKIN ET AL.	
	Examiner	Art Unit	
	Matthew T Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 November 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1-18* is/are rejected.

7)☒ Claim(s) *1-7, 14-18* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 November 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

This action is in response to the communication filed on November 29, 2000.

DETAILED ACTION

1. Claims 1-18 have been examined.

2. The Art Unit location of your application in the USPTO has changed. To aid in correlating any papers for this application, all further correspondence regarding this application should be directed to Art Unit 2131.

Title

3. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

4. The following title is suggested: *Message Digest Hardware Accelerator Including SHA-1 and MD5 Implemented Therein.*

Priority

5. No foreign priority has been claimed in this application.

6. The effective filing date of the subject matter defined in the pending claims of this application is 11/29/2000.

Information Disclosure Statement

7. No information disclosure statement has been submitted.

Drawings

8. The drawings submitted on 11/29/2000 are acceptable for examination proceedings.

Specification

9. The abstract of the disclosure is objected to because of the following informalities:

Line 1: "Message Digest Hardware Accelerator" must be removed, as it is not a proper heading for the Abstract of the Disclosure.

Correction is required. See MPEP § 608.01(b).

Claim Objections

10. Claims 1-7, 14-18 objected to under 37 CFR 1.75 because of the following informalities:

Claims 1-7, 14-18 recite "message digest hardware accelerator" in each preamble. This phrase does not convey the nature of the invention and the examiner suggests changing the phrase to "apparatus".

Appropriate correction is required. See MPEP § 608.01(i).

Claim Rejections - 35 USC § 112

11. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> *The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.*

12. Claims 15, 16, and 17 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 15 recites the limitation "the sixteen registers" in Line 3. There is insufficient antecedent basis for this limitation in the claim.

13. Claim 16 is rejected by virtue of its dependency on claim 15.

14. Claim 17 recites the limitations "the register array" and "the word wise circular queue" in Line 2. There is insufficient antecedent basis for these limitations in the claim.

Claim Rejections - 35 USC § 103

15. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> *(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

16. Claims 1-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ober et al. (U.S. Patent Number 6,708,273) hereinafter referred to as Ober, in view of Childs et al. (U.S. Patent 5,623,545) hereinafter referred to as Childs, Schneier (Applied Cryptography) hereinafter referred to as Schneier, Turner et al. (U.S. Patent Number 4,896,296) hereinafter referred to as Turner, and further in view of Batcher (U.S. Patent Number 4,314,349) hereinafter referred to as Batcher.

Ober disclosed an integrated circuit for performing security functions including the SHA-1 and MD5 hash algorithms (See Ober Figure 1 Element 30). However, Ober failed to disclose an embodiment for the implementation of the two hash functions.

Childs teaches a hardware implementation of the SHA-1 algorithm. The implementation includes five registers for storing chaining variables as called for by the SHA-1 algorithm (See Childs Fig. 5 elements 508-512). Childs teaches a function circuit receiving chaining variables B, C, and D (See Childs Fig. 5 Element 516). Childs also teaches a summing circuit (Elements 520-523) receiving the output of the function circuit (f_e) and the fourth chaining variable (E) and the output coupled to the register file through a multiplexer (Element 507) (See Childs Fig. 5).

Schneier teaches that the MD5 algorithm has the same elements shown above for the SHA-1 algorithm, except that there is not a fifth chaining variable 'E' as in SHA-1 (See Schneier Page 438 Fig. 18.6).

Turner teaches that by using a multiplexer, with one input set to zero, the other inputs can be selectively excluded from the input to another function (See Turner Col. 7 Paragraph 4).

Batcher teaches that multiplexers can be implemented in order to minimize the number of elements of a circuit (See Batcher Col. 6 Paragraph 3).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Childs and Schneier in the invention of Ober in order to carry out the hashing functions. This would have been obvious because one of ordinary skill in the art would have been motivated to provide the full functionality of the IPSec protocol when implementing this protocol.

It also would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Turner in the combination of Ober, Childs, and Schneier in order to selectively exclude the fifth chaining variable (E) from the inputs to the summing circuit. This would have been obvious because one of ordinary skill in the art would have been motivated to utilize the multiplexer in order to minimize the elements in the circuit of Ober.

17. Claim 2 recites a barrel shifter, coupled to an adder, coupled to a multiplexer, all coupled to the output of the summing circuit. MD5 requires a shifter and adder coupled to the output of the summer, as can be seen in the two rightmost elements of figure 18.6 (See Schneier Page 438). Claim 2 further recites the other input of the multiplexer being coupled to the output of the summing circuit. SHA-1 does not require the shifter or the adder at the output of the summing circuit.

It would have been obvious to employ the teachings of Batcher in order to multiplex the elements of the SHA-1 algorithm and the MD5 algorithm in order to minimize the elements in the Hash Block of Ober.

18. Claim 3 recites a third multiplexer coupled to the output of the second multiplexer and also coupled to the register file to receive a fifth chaining variable (A). Childs disclosed that chaining variable B had input from chaining variable A during SHA-1 (See Childs Fig. 5 Elements 508 and 509). Schneier disclosed that chaining variable B had input from the result of the adder (See Schneier Page 436 Paragraph 9 – Page 437 Paragraph 1).

Claim 3 further recites a fourth multiplexer coupled to the output of the second multiplexer and to the register file for receiving the third chaining variable (D). Childs disclosed that chaining variable A had input from the summing circuit during SHA-1 (See Childs Fig. 5 Elements 507, 508, and 523). Schneier disclosed that chaining variable A was coupled to the chaining variable D (See Schneier Page 437 Lines 18-21).

It would have been obvious to employ the teachings of Batcher in order to multiplex the elements of the SHA-1 algorithm and the MD5 algorithm in order to minimize the elements in the Hash Block of Ober.

19. Claims 4-5 were inherent in the combination of Ober, Childs, Schneier, Batcher and Turner, in order for proper operation of the MD5 and the SHA-1 when each was selectively performed in Ober. This was inherent because the MD5 algorithm must have received the correctly multiplexed inputs for MD5 and the SHA-1 must have received the correctly multiplexed inputs for SHA-1 in order for the hashes to be calculated correctly.

20. Regarding claim 6, Childs disclosed a shift circuit and a fifth multiplexer for selectively shifting the second chaining variable (B) for input to the third chaining variable (C) (See Childs Fig. 5 Elements 509, 518, 517, and 510).

21. Regarding claim 7, Childs disclosed a shift circuit receiving chaining variable A and outputting to the summing circuit in accordance with SHA-1 (See Childs Fig. 5 Elements 508, 519, 520, and 522). Schneier disclosed chaining variable A being input to the summing circuit in accordance with MD5 (See Schneier Figure 18.6).

It would have been obvious to employ the teachings of Batcher in order to multiplex the elements of the SHA-1 algorithm and the MD5 algorithm in order to minimize the elements in the Hash Block of Ober.

22. Claim 8 recites a storage circuit (See Childs Fig. 5 Element 515), a register array providing W_t (See Childs Fig. 5 Element 514), a register file for storing chaining variables A-E (See Childs Fig. 5 Elements 508-512), and a summing circuit (See Childs Fig. 5 Elements 520-523) receiving constants from the storage circuit (See Childs Fig. 5 Elements 515 and 520), one input coupled to the register array (See Childs Fig. 5 Elements 514 and 520), one input coupled to either chaining variable A or a shifted version of chaining variable A depending on the mode of operation (See rejection for claim 7 above), one input for receiving a logical function in accordance with chaining variables 1, 2, and 3 (See Childs Fig. 5 Element 516), and one input providing a fourth chaining variable or a zero depending on the mode of operation (See rejection of claim 1 above).

Claim 8 further recites the storage circuit storing two sets of constants, one for SHA-1 and one set for MD5. Childs disclosed storing the set K_t for SHA-1 (See Childs Fig. 5 Element 515 and Col. 8 Paragraph 3) and although Schneier did not specifically disclose storing the constants for MD5, it was inherent that they were stored in order to have performed the 64 steps in the four rounds as required by the MD5 algorithm (See Schneier Pages 438-440 t_i).

It would have been obvious to employ the teachings of Batcher in order to multiplex the constants of the SHA-1 algorithm and the MD5 algorithm in order to minimize the elements in the Hash Block of Ober.

23. Claim 9 rejected for the same reasons as claim 1 as applied to claim 8 above.

24. Claim 10 rejected for the same reasons as claim 2 as applied to claim 9 above.

25. Claim 11 rejected for the same reasons as claim 3 as applied to claim 10 above.

26. Claim 12 rejected for the same reasons as claim 6 as applied to claim 11 above.

27. Claim 13 rejected for the same reasons as claim 7 as applied to claim 12 above.

28. Claim 14 recites a register file for storing five chaining variables, in which the five variables are preloaded for each of two algorithms. Childs depicted a register file for storing five chaining variables (See Childs Fig. 5 Elements 508-512) and also disclosed loading the registers with preset values at the beginning of the SHA-1 algorithm (See Childs Fig. 5 Element 507 and Col. 1 Lines 25-32). It was inherent in the combination of Ober, Childs, Schneier, Batcher and Turner, that when MD5 was being performed, the initial MD5 variables were loaded into the register file (See Schneier Page 436 Lines 33-38).

Claim 14 further recites a function circuit receiving three of the chaining variables and producing a logical value dependant on the algorithm being performed. Childs disclosed a function circuit taking three chaining variables and producing a logical value for the SHA-1 algorithm (See Childs Fig. 5 Element 516). Schneier disclosed a function, for the MD5 algorithm, which took three chaining variables and produced a logical output (See Schneier Page 437 Lines 5-11). These functions are different for SHA-1 and MD5 (See Childs Col. 1 Table at Line 20 and Schneier Page 437 Lines 5-11).

Claim 14 also recites a storage element for providing a set of constants for each algorithm to a summing circuit, and the summing circuit also receiving the output of the function circuit (See rejection of claim 8 regarding the storage circuit).

29. Claim 15 recites a register array, with sixteen registers and a decoder circuit for selecting a word from the register array for the first algorithm (See Childs Fig. 6 Elements 602, and 603 and Schneier Page 437 Line 16 – Page 440 Line 17).

30. Claim 16 recites the register array forming a word wise circular queue (See Childs Fig. 6 Elements 602, 603, 605, 608, and 601), an exclusive-OR receiving four data words from the register file (See Childs Fig. 6 Elements 603, 605, and 606), and a shift register coupled to the output of the exclusive-OR for providing input to the register file (See Childs Fig. 6 Elements 605, 607, 608, 601, and 602). Claim 16 further recites the shift being a one-bit shift (See Childs Abstract).

31. Claim 17 recites an output of the array being supplied from a word-wise circular queue when computing a second algorithm (See Childs Fig. 6 Element 602, 603, and 604).

32. Claim 18 recites the first algorithm being MD5 and the second algorithm being SHA-1. Schneier disclosed the first algorithm being MD5 (See Schneier Page 436) and Childs disclosed the second algorithm being supplied by FIPS PUB 180-1 (See Childs Abstract), which is the SHA-1 algorithm.

Conclusion

33. Claims 1-18 are rejected.

34. Any inquiry concerning this communication should be directed to Matthew Henning whose telephone number is (703) 305-0713. The examiner can normally be reached Monday-Friday from 9am to 4pm, EST.

If attempts to reach examiner by telephone are unsuccessful, the examiner's acting supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The fax phone number for this group is (703) 305-3718.

Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (703) 305-3900.

Matthew Henning
Assistant Examiner
Art Unit 2131

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100